2361 ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES (M)

M

PURPOSE

The Palmyra Board of Education recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, the Palmyra Public School District will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in school. The district's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their lives. The guidelines prescribed in this document are driven out of deference to four guiding principles: respect, privacy, sharing, and safety.

POSITION STATEMENT

Recognizing that school policies need to be adaptable to the times, the BOE believes that the revision process should be ongoing to accommodate new technologies and educational trends.

The Palmyra Public School District provides access to electronic resources that promote educational excellence, sharing of information, innovative instruction, and online communication to enhance 21st century learning and living. Online communication constitutes, but is not limited to, Internet, Email, Podcasting, and Blogging. Electronic resources include, but are not limited to hardware, software, data, printers, servers, filtered Internet access, local and wide area networks, wireless networks, and communication devices such as cell phones, and mobile devices including laptops, tablets and flat screen interactive boards.

COMPLIANCE

The school district is in compliance with the Children's Internet Protection Act (CIPA) and has installed technology protection measures for all computers in the schools. These measures allow for blocking and/or filtering content that is considered obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other visual depictions that taken as a whole and with

respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors; sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.

RESPONSIBLE USE

Acceptable/responsible network use by students and staff includes, but is not limited to:

- Access libraries, databases or other Internet sites provided by your teacher
- Complete and return assignments via email and the district Google domain.
- Create files, projects, videos, web pages and podcasts for projects
- With permission, publish your work on the web

- Participate in approved blogs, wikis, social networking sites, and bulletin boards
- Use email and instant messaging to contact teachers
- Downloading online study aids
- Participate in virtual classes
- Make world-wide connections
- Read e-books

Acceptable/responsible network use by staff includes, but is not limited to:

- Appropriate classroom webpage design
- Proper use of network to support education and research
- Use of the network for incidental personal use in accordance with all district policies and guidelines
- Email for student/parent communication only (no personal use)
- Incorporation and creation of blogs, podcasts, video conferencing, online collaborations, texting or other forms of electronic communications (i.e. cell phones, cameras) or web applications for educational purposes
- Professional Development opportunities

Unacceptable network use by students and staff includes, but is not limited to:

- Downloading, installation and use of games, audio files, video files or other applications (including shareware and freeware) without permission or approval from an authority
- Hacking, cracking, vandalizing, the introduction of viruses, worms, or other malicious software onto any network equipment

- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks
- Information posted, sent or stored online that could endanger others
  Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material
- Sharing personal information and network credentials with others
  Copyright infringement
- Attaching unauthorized equipment to the district network

Palmyra students and staff use the Internet to participate in distance learning activities, to ask questions of and consult with experts, to communicate with other students and individuals worldwide, and to locate material to meet their educational information needs. The use of the Internet is a privilege, not a right. Inappropriate use may result in a cancellation of privileges. Our educational staff has a professional responsibility to work together to help students develop the intellectual skills needed to discriminate among informational sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information obtained electronically to help meet their educational goals.

In accordance with Bill A592, the district web site will not disclose any personally identifiable information about a student without receiving prior written consent from the student's parent or legal guardian on a form developed by the Department of Education. As used in this act, "personally identifiable information" means student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.

EXPECTED BEHAVIOR

Students and staff are expected to demonstrate responsible behavior on the district computer network and all related hardware and software, just as they are in any instructional or non-instructional setting within the district.

Passwords and account information are not to be shared among staff or students for any accounts, WAN and cloud.

The use of the Internet is a privilege. Students and staff are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

1. Be polite. Do not get abusive in your messages to others. Use appropriate language. Do not swear; use vulgarities or other inappropriate language. Illegal activities are strictly forbidden.

2. Do not reveal your own personal address or phone number or that of students or colleagues. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or support of illegal activities may be reported to the authorities. Do not use the network in such a way that you would disrupt the use of the network by other users. All communications and information accessible via the network should be assumed to be private property. You may not attempt to use or alter anyone else's network account. You may not break in or attempt to break into other computer systems. You may not create or share computer viruses. You may not destroy another person's data. Transmission or reception of any material in violation of an U.S. or State regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. The district WAN has multiple security layers including cloud protection and services. However, responsible user behavior is the most critical layer.

The Palmyra School District maintains certain policies with regard to the use and security of its system. The Board reserves the right to log use of telecommunications and network use and to monitor file server space utilization by users. Network storage areas will be treated like school lockers as described in the district's search and seizure policy. They remain the sole property of the district and are subject to administrative search, by school officials, at any time, in the interests of school safety, discipline, enforcement of school rules and regulations and enforcement of the law. Any search of the aforesaid items by law enforcement officials shall only be conducted upon presentation of a proper search warrant. All users of our facilities are expected to be familiar with these policies.

Violations of this policy can lead to the suspension of a computer account pending investigation of circumstances. Serious violations of this policy will be referred directly to the appropriate academic or outside authorities. Unauthorized use of district computing facilities can be a criminal offense. The penalties may be as severe as suspension or dismissal from the district and/or criminal prosecution. In addition, students may be held financially responsible for any damage or destruction to the network or equipment.

TERMS AND CONDITIONS

1. Students should be monitored at all times by instructional staff.

2. Unauthorized attempts to gain privileged access or access to any account not belonging to you on any district system is not permitted.

3. Individual accounts cannot be transferred to or used by another individual. Sharing passwords is not permitted.

4. Each user is responsible for all matters pertaining to the proper use of their account; this includes choosing safe passwords.

5. It is the student's responsibility to become familiar with the rules and procedures regarding the district policies involving use of the district network.

6. No district system may be used as a vehicle to gain unauthorized access to other systems.

7. No district system may be used for commercial or for profit activities. Use for product advertisement or unauthorized political lobbying is also prohibited.

8. No district system may be used for unethical, illegal, or criminal purposes.

9. Any user who finds a possible security lapse on any district system is obliged to report it to an administrator. Don't attempt to use the system under these conditions until the administrator has investigated the problem.

10. Please keep in mind that many people use the district systems for daily work. Job related activities always take precedence over any personal activities.

11. Electronic mail on all district systems is as private as we can make it. Attempts to read another person's electronic mail or other protected files will be treated with the utmost seriousness. The system administrators will not read mail or non-word-readable files unless deemed necessary in the course of their duties, and will treat the contents of those files as private information at all times.

12. Use of the district system for commercial uses, except by approved outside organizations, is strictly prohibited. Such prohibited uses include, but are not limited to, development of programs, data processing or computations for commercial use and preparation and presentation of advertising material.

13. Students are not permitted to use electronic mail and other forms of direct electronic communication unless engaged in an instructional activity sanctioned and monitored by an instructional staff member.

14. The school district does not condone or tolerate the unauthorized copying or use of licensed computer software. You must adhere to the district's contractual

responsibilities and comply with all copyright laws. Anyone who violates this policy may be subject to immediate suspension of system access pending investigation by the Principal/Technology Supervisor. An individual engaged in the unauthorized copying or use of software may also face civil suit, criminal charges, and/or penalties and fines. Subject to the facts and circumstances of each case, such individuals shall be solely responsible for their defense and any resulting liability.

15. No district system may be used for sending nuisance messages, such as chain letters and obscene or harassing messages.

16. The Children's Internet Protection Act does not permit an administrator or supervisor or "person authorized" to disable the technology protection measure to enable access for bona fide research or other lawful purpose.

17. All students and staff members will be oriented regarding these policies and procedures at the beginning of every school year.

18. All network activities are subject to the aforementioned rules and regulations.

19. All the above pertain to both students and all school district personnel.

The district may modify these rules at any time by publishing the modified rule(s) on the system.

N.J.S.A. 2A:38A-3
Federal Communications Commission: Children's Internet Protection Act.

NEW TECHNOLOGIES – MOBILE DEVICES
Mobile devices include such equipment as cell phones, laptops, and tablets. It should be understood by all parties that communication on such devices cannot be considered private when used within the school district or when used anywhere to communicate with other parties during discussions about school.

Remote Learning and Instruction
While utilizing district distributed technology away from school grounds, students and staff should continue to follow all of the instructions outlined above. All users should also be aware that these devices will be under 24/7 monitoring by either administrative staff or pre-installed monitoring software.

Use of Student Mobile Devices at School or School-Sponsored/Related Activities
When Mobile Devices are misused, students will be subject to disciplinary action including, but not limited to, verbal or written warnings, denial of the privilege of

participating in extracurricular and athletic activities, suspension from school, expulsion from school, and taking away the Mobile Device. When Mobile Devices are taken away by school personnel, the Mobile Device will be retained until the end of the school day and then returned to the student. Depending upon the seriousness of the offense, further possession of the Mobile Devices at school may be denied for a time period determined by the school administration.
Students who misuse Mobile Devices in any of the following ways may face disciplinary action:

- Refusal to Turn Off a Mobile Device
  Students in possession of a Mobile Devices must turn it off when directed by a teacher, administrator, coach, counselor, or other school personnel.

- Cheating
  Students may not use Mobile Devices in or out of the classroom to get or give answers to tests, to copy information available on the internet and submit it as the student's own work, or to engage in any similar form of electronic cheating.

- Cyberbullying
  Bullying means threatening another person by words (name-calling, disrespect, shunning) or by physical force (pushing, shoving, restraining).

  Cyberbullying refers to bullying that is done electronically through Mobile Devices and that causes physical or emotional harm to the victim, or disrupts school activities. This form of bullying may either be sent directly to the victim or indirectly through messages sent to others. This includes, but is not limited to, blogging and posting on social networking sites.

- Harassment
  Spoken, written, or graphic attacks against someone made in person or through the use of Mobile Devices that materially disrupt classwork, cause substantial disorder, or create a hostile educational environment for school personnel or students is known as harassment.

- Harassment because of a person's race, color, religion, ancestry, national origin, gender, sexual orientation, medical condition, or disability is illegal and absolutely prohibited.

- Disruption of School Activities
  Disruption of school activities occurs:

  If instruction or educational activities are significantly interrupted,

Students and educational personnel are denied access to or cannot focus on classroom or out-of-classroom activities, or
Continuous disciplinary measures are necessary to maintain order and protect persons and property from harm.

- Sexting
  Sexting means taking, sending, forwarding or asking to receive messages, photos, or videos of persons who are partially or completely undressed or are pretending to or actually performing a sexual act.

- Threats
  Students may not use Mobile Devices to communicate a serious intent to harm or assault students or school personnel.

Revised: 14 August 2012
Revised: 12 June 2019
Reviewed: 13 November 2019
Revised: 26 August 2020

Palmyra Student Agreement

Please find and read the attached Policy 2361. This policy is available in the Superintendent's Office at Delaware Avenue School. This policy is also available on the District Website. If you have any questions please see the appropriate person in your school building.

Refusal to sign-off on the above referenced Policy mandates the following:

You may not use any equipment or infrastructure on the District computer network, including, but not limited to, all computers, printers, scanners, projectors, flat screen interactive boards, cameras, network drops, or mobile devices at any time for any reason.

I, _____, a student at Palmyra Public Schools, am aware of the significant responsibilities associated with the use of information technology and the Internet and that my behavior while using the computer network may be monitored. I understand that if I do not adhere to this policy and guidelines I may be restricted or lose my network privileges which could result in disciplinary action. I agree to:

- Use the District technology resources for educational purposes only
- Treat with respect and exercise reasonable care in using network technology resources
- Keep my personal information and passwords secure and not trespass in another's personal network space
- Avoid tampering with software and hardware on school district equipment
- Proceed with responsible behavior in all aspects of my work with the school district network resources.

My signature below indicates that I understand the expectations as set forth in the Responsible/Acceptable Use Policy referenced above including the guidelines listed on this page.

_____
Student Name (Print)

_____ _____
Student Signature Date

_____ _____
Parent/Guardian Signature Date

Palmyra Staff Agreement

Please find and read the attached Policy 2361. This policy is available in the Superintendent's Office at Delaware Avenue School. This policy is also available on the District Website. If you have any questions please see the appropriate association representative in your building.

Refusal to sign-off on the above referenced Policy mandates the following:

You may not use any equipment or infrastructure on the District computer network, including, but not limited to, all computers, printers, scanners, projectors, SMART Boards, cameras, network drops, or mobile devices at any time for any reason.

I, _____, a staff member at Palmyra Public Schools, am aware of the significant responsibilities associated with the use of information technology and the Internet. I certify that I have read the attached Policy and understand the manner in which I am bound to suitable behavior. Specifically, I agree to:

- Use the District technology resources for educational purposes only
- Treat with respect and exercise reasonable care in using network technology resources
- Keep my personal information and passwords secure and not trespass in another's personal network space
- Avoid tampering with software and hardware on school district equipment
- Proceed with responsible behavior in all aspects of my work with the school district network resources

My signature below indicates that I understand the expectations as set forth in the Responsible/Acceptable Use Policy referenced above including the guidelines listed on this page.

_____ _____

Staff Signature Date

Please be advised that a copy of this page and your signature will be placed in your personnel file.

Internet Release Form – Palmyra Public Schools

In order for a student to access the Internet and use the technological resources at Palmyra Public Schools, a parent/guardian and the student must sign and return a copy of the Responsible/Acceptable use Policy as well as this consent form.

_____ I GIVE my permission for Palmyra Public Schools to allow my child computer access to the Internet and my child agrees to the usage guidelines listed herein.

_____ I DO NOT GIVE my permission for Palmyra Public Schools to allow my child computer access to the Internet. Since the school cannot always prevent student access to such services, I have directed my child not to access said services.

Electronic Release

_____ I give permission to display my child's image at school or on the District website.

_____ I give my permission to display my child's voice at school or on the District website.

_____ I give permission to display my child's work at school or on the District website.

_____ I do not want my child's image to be displayed at school or on the District website.

_____ I do not want my child's voice to be displayed at school or on the District website.

_____ I do not want my child's work to be displayed at school or on the District website.

Parent Signature _____ Date _____